## Amendments to the Claims

1. (original) A method of establishing a consistent password policy, said method comprising:

describing a plurality of password policies in a computer usable password policy data structure;

accessing said computer usable password policy data structure by a password policy enforcement agent; and

enforcing at least one of said plurality of password policies described within said password policy data structure by said password policy enforcement agent.

2. (currently amended) The method of Claim 1 wherein said computer usable password policy data structure comprises a file structure ~~substantially~~ compatible with extensible markup language.

3. (original) The method of Claim 1 wherein said password policy enforcement agent is operable on a client computer of a client-server computer system.

4. (currently amended) The method of Claim 1 wherein said method is operable on a utility data center.

5. (original) The method of Claim 1 further comprising validating said computer usable password policy data structure for authenticity by said password policy enforcement agent.

6. (original) The method of Claim 1 wherein said plurality of password policies comprises a threshold parameter for unsuccessful access attempts that when exceeded disables a computer system access account.

7. (currently amended) The method of Claim 6 wherein said plurality of password policies comprises a parameter indicating ~~the~~ a time duration, and wherein exceeding said threshold parameter ~~within which said threshold parameter number of unsuccessful access attempts~~ triggers locking of a computer system access account within said time duration.

8. (original) The method of Claim 1 wherein said plurality of password policies comprises an initial delay parameter to block access to a computer system access account for a period of time after an unsuccessful access attempt.

9. (currently amended) The method of Claim 8 wherein access to said computer system access account is delayed for an increasing time period for successive unsuccessful access attempts.

10. (original) The method of Claim 1 wherein said plurality of password policies comprises a minimum password length parameter.

11. (original) The method of Claim 1 wherein said plurality of password policies comprises a maximum password length parameter.

12. (currently amended) The method of Claim 1 wherein said plurality of password policies comprises a parameter ~~to prohibit passwords consisting of a natural language word~~ for prohibiting passwords comprising a word associated with a natural language.

13. (currently amended) The method of Claim 12 [[1 ]]wherein said natural language is English.

14. (currently amended) The method of Claim 1 wherein said plurality of password policies comprises a parameter for prohibiting ~~to prohibit~~ passwords comprising ~~consisting of~~ a palindrome.

15. (currently amended) The method of Claim 1 wherein said plurality of password policies comprises a parameter for prohibiting ~~to prohibit~~ passwords comprising ~~consisting of~~ a derivative of a computer system account name.

16. (currently amended) The method of Claim 1 wherein said plurality of password policies comprises a parameter for ~~to~~ automatically generating ~~generate~~ a password.

17. (currently amended) The method of Claim 1 [[16 ]]wherein said plurality of password policies comprises a parameter for ~~to~~ automatically generating ~~generate~~ a pronounceable password consistent with ~~all of~~ said plurality of password policies.

18. (currently amended) The method of Claim 1 [[16 ]]wherein said plurality of password policies comprises a parameter for specifying ~~to specify~~ a set of characters utilizable to automatically generate a password.

19. (currently amended) The method of Claim 1 further comprising providing, by said password policy enforcement agent, feedback to a configuration and aggregation point, about whether said at least one of said plurality of password policies ~~which of said plurality of password policies have~~ has been successfully enforced.

20. (currently amended) ~~A computer usable password policy data structure comprising computer access password policy parameters.~~

Instructions on a computer usable medium wherein the instructions when executed cause a computer system to perform a method of establishing a consistent password policy, said method comprising:

describing a plurality of password policies in a computer usable password policy data structure;

providing an access point with access to said computer usable password policy data structure; and

receiving feedback from a password policy enforcement agent associated with said access point about which of said plurality of password policies have been successfully enforced.

21. (currently amended) The computer usable medium of Claim 20 wherein said computer usable password policy data structure ~~of Claim 20 comprising~~ comprises a file structure ~~substantially~~ compatible with extensible markup language.

22. (currently amended) The ~~computer usable password policy data structure of Claim 20 comprising a computer access password policy parameter selected from the set of computer access password policy parameters comprising~~ computer usable medium of Claim 20 wherein said method further comprises:

selecting a computer access password policy parameter from said plurality of computer access password policy parameters consisting of a parameter selected from a group of parameters comprising a threshold parameter for unsuccessful access attempts that when exceeded disables a computer system access account[[;]], a parameter indicating the a time duration within which said threshold parameter number of unsuccessful access attempts triggers locking of a computer system access account[[;]]; an initial delay parameter to block access to a computer system access account for a period of time after an unsuccessful access attempt[[;]], a minimum password length parameter[[;]], a maximum password length parameter[[;]], a parameter to prohibit passwords consisting of a natural language word[[;]], a parameter to prohibit passwords consisting of a palindrome[[;]], a parameter to prohibit passwords consisting of a derivative of a computer system account name[[;]], a parameter to automatically generate a password[[;]], a parameter to automatically generate a pronounceable password consistent with all of said plurality of password policies[[;]], and a parameter to specify a set of characters utilizable to automatically generate a password.

23. (currently amended) A computer system comprising:

a computer usable password policy data structure comprising a plurality of password policies; and

a server configured to provide access to said computer usable password policy data structure at an access point configured to enforce at least one of said plurality of password policies using a password policy enforcement agent.

~~a first server computer for controlling access to said computer system;~~

~~a second server computer coupled to said first server computer for providing control of said computer system;~~

~~computer usable media comprising computer usable instructions than when executed on a processor of said first server computer implement a method of establishing a consistent password policy, said method comprising:~~

~~accessing a computer usable password policy data structure; and~~

~~enforcing a password policy described within said password policy data structure.~~

24. (original) The computer system of Claim 23 comprising a utility data center.